Assessing Security Risk and Requirements for Systems of Systems

Duncan Ki-Aries
Bournemouth University
Fern Barrow, Poole, UK
dkiaries@bournemouth.ac.uk

***Abstract*—A *System of Systems* (SoS) is a term used to describe independent systems converging for a purpose that could only be carried out through this interdependent collaboration. Many examples of SoSs exist, but the term has become a source of confusion across domains. Moreover, there are few illustrative SoS examples demonstrating their initial classification and structure. While there are many approaches for engineering of systems, less exist for SoS engineering. More specifically, there is a research gap towards approaches addressing SoS security risk assessment for engineering and operational needs, with a need for tool-support to assist modelling and visualising security risk and requirements in an interconnected SoS. From this, security requirements can provide a systematic means to identify constraints and related risks of the SoS, mitigated by human-user and system requirements. This work investigates specific challenges and current approaches for SoS security and risk, and aims to identify the alignment of SoS factors and concepts suitable for eliciting, analysing, validating risks with use of a tool-support for assessing security risk in the SoS context.**

***Index Terms*—System of Systems, Security, Risk, Requirements Engineering, System of Systems Engineering.**

I. Project Motivation and Scope

Independent systems may at times need to come together to achieve a greater or combined purpose in a collaborative nature. For example, an emergency response unit may need to manage and interoperate with the police, fire, ambulance, or other critical services. Each of these may be considered an independent system with its own purpose, people, processes and technology, yet when collaborating with the emergency response unit, this is to meet emergency response mission objectives. This example of systems coming together for a greater interaction collaborating with the emergency response unit can be described as being a System of Systems (SoS). Other examples of SoS may be less or more complex, or have differing levels of management, control, and constraints affecting the SoS as a whole; greater than that of a single system, of which may also be different or conflicting at times.

Accounting for SoS security risk is dependent upon what or whose view is being assessed within the SoS. Security risk in SoSs is challenged by differing goals, trust boundaries and levels of assurance, potentially leading to conflicting human and system requirements across the interconnected SoS. Moreover, each entity may only know or have access to varying levels of information about other systems in which to assess and model security risk at the SoS level. In some scenarios, a SoS may have limited or no central management, or a weak collaboration with minimal or no useful information to support security risk assessments, presenting further obstacles towards the elicitation of suitable security requirements addressing security needs and concerns within the independent systems and the SoS as a whole.

Broad research discussing SoSs exists, but lacks in suitable case-studies to support the topic of security risk assessment in SoSs. Furthermore, there is very little that demonstrates modelling and visualisation of security risks, people, process and technology for SoSs and requirements engineering. Current tools appear to be designed with a single system or organisation in mind, thus scaling-up to a SoS, sometimes of which can be quite complex requiring many designs, is a challenge. Identifying suitable combinations of tools and techniques appropriate for modelling and visualising these SoS interactions would therefore be useful to assist the SoS security risk assessment and requirements engineering process. The scope of this research project will therefore apply focus towards security risk assessment in SoSs from the operational view transitioning to systems and SoS security requirements engineering considerations to further model, assess and mitigate against risk. This will use research and case-studies to explore suitable repeatable methods and approaches for a security risk assessment in SoSs, using a tool-supported framework to assist with risk-based decision making.

Research questions in Section II provided structure for identifying challenges associated with assessing and modelling security risk and requirements in a SoS, and continues to be applied using methods described in Section III. A summary of related research is discussed in Section IV providing a foundation for identifying current approaches that frame SoSs, and their challenges, human factors, security risk and modelling approaches. An overview of project contributions is summarised in Section V discussing related work towards research questions [1][2][3], followed by a summary and next steps in Section VI.

II. Research Questions

When considering preliminary research, there appear to be gaps between SoSs frameworks or industry approaches towards how security risk may be modelled, visualised and assessed within a SoS context. To address this research gap, research questions (RQs) focus on three core areas of consideration for SoS security risk and requirements:

RQ1 What SoSs factors contribute to challenges of security risk assessment of SoSs?

RQ2 What concepts are suitable to support a framework for security risk assessment with requirements elicitation in SoSs?

RQ3 How can the SoS security risk assessment framework be extended using modelling and visualisation software tools to assist the SoS security risk and requirements process?

III. Research Methods

To address research questions, a qualitative approach is taken combining inductive and deductive methods with action research, e.g. with the creation and refinement of the approach with case-studies to investigate and identify SoS challenges for security risk and requirements. Using Grounded theory to systematically analyse data will further assist research and case-studies forming a theory from its output, supported by literature reviews, interviews or focus groups with relevant stakeholders to ground the theory based on the empirical study. Prototyping will be used in differing scenarios to address RQ2 and RQ3, for example, where SoS elements are implemented into a suitable risk assessment process, then modified and tested with tool-support. Elements of interpretive design are to be explored within this part agenda-driven research, where general scope for future work is identified, taking a model-driven approach towards security risk and requirements engineering. SoS case-studies and exemplars are, however, a central focus for RQ's to help test, validate and formalise the framework blending a component-driven and system-driven risk assessment approach, using tool-support to model and assess SoS security risk and requirements.

IV. Related Work

A. Risk in Security

Risk in a security context can be defined as the effect of uncertainty on objectives [4]. Describing security risk can be synonymous with information technology related risk, considering the probability and impact of a threat-source intentionally or accidentally exploiting a system or information asset vulnerability [5]. The combination of the probability and impact equates to the level of risk present. Security is about the protection of assets from threats and vulnerabilities, applying security controls to reduce or mitigate risk [6]. We can define an *Asset* as anything that has value to the organisation; A *Threat* as a potential for a threat-source to accidentally trigger or intentionally exploit a specific vulnerability; and a *Vulnerability* as a weakness in system security procedures, design, implementation, or internal controls that could result in a security breach or a violation [4][7]. Threat impact may derive from unauthorised disclosure, modification, or destruction of information, failure to exercise due care and diligence in the implementation and operation, unintentional errors, omissions, or disruptions due to natural or man-made disasters [5].

Information Security processes, controls and methodologies protect print, electronic, or any other form of confidential, private and sensitive information or data [8]. These should also consider needs of training and awareness, physical security, due diligence on third parties and contractual management, and data privacy requirements [9]. Documenting risk should be written in business-friendly language rather than endless detail of overly complex technical jargon, and be presented under high-level headings noting potential impacts on operations [10]. A range of risk approaches may be used, although in the current context, it is expected that risk assessment should at the very least use modelling, and be repeatable, measureable, and auditable [11]. A number of differing methods for security risk management exist, e.g. [4][12], covering a wide range of security techniques, controls and considerations towards security protection. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology is another that stands out, offering three approaches requiring differing levels of skill and application. The OCTAVE Allegro iteration is suitable for assessing Information Security risk, reducing the need for participatory workshops from all organisational and levels, whilst producing more robust results without the need for extensive risk assessment knowledge [13].

B. System of Systems and Systems Risk

Before exploring where SoS security risk assessment is challenged, it is useful to consider how the term *System of Systems* applies, and the context in which *System* is used, e.g. the coming together of people, process, software and hardware, integrated to achieve a purpose. Systems are composed of parts or elements with relationships between other elements of the system [14]. However, the arrangement of the whole must be understood to appreciate how the system is formed [15]. Some may also be regarded as socio-technical systems - organisational systems that include people, processes and technological systems, where intrinsic complexity arises from the multi-dimensional interactions [16] of which creates greater challenges when scaled-up into a SoS environment.

Historically, SoSs are considered to be large-scale concurrent and distributed systems, comprised of complex systems with autonomy [17][18], yet equally a SoS is a system that contains two or more independently managed elements [14], regardless of scale. The SoS concept may therefore mean different things to different people. In an organisational context, the SoS is the enterprise-wide sharing of core business information across functional and geographical areas. Whereas, military and defence SoSs can be configurable sets of constituent-systems in dynamic communication infrastructures [19]. A SoS could therefore be described as consisting of multiple, heterogeneous, operationally, distributed, occasionally independently, operating systems embedded in networks at multiple levels that evolve over time [20]. The coming together provides a set of systems for a task that none of the systems can accomplish on their own. However, each constituent system keeps its own management, goals, and resources while coordinating within the SoS and adapting to meet SoS goals [21]. SoS examples include smart devices to smart cities, and many Internet of Things (IoT) systems, general business information systems, sensor networks emergency response units, defence

and national security, and many more [1][2][22]. Aligning with other research of SoSs, we can simply define a *System of Systems* as being *'the coming together of independent systems collaborating for a new or higher purpose'* [3]. Within the limited range of SoS-based engineering guides and literature, many reproduce SoS descriptions and definitions largely founded and supported by Maier [23] along with Dahmann and Baldwin [24], bringing together the main four summarised categories of SoSs.

- *Directed SoSs* possess central management, operation and control over the SoS as a whole;
- *Acknowledged SoSs* have designated management, but limited control over the SoS as a whole;
- *Collaborative SoSs* have no central management, so operation and control is formed and agreed as a mutual independent collaboration;
- *Virtual SoSs* have individual independent collaboration with no central management, operation or control of the SoS as a whole.

While SoSs generally fall into one of these categories, the distinction is not always clear. In some scenarios, a system within the SoS may also be considered as a type of SoS within its own operational environment. These SoSs are often composed of independent systems and sub-systems, coming together in ways elements may not have originally been designed for. Emergence can be described as relating to the formation of new behaviours due to development or evolutionary processes and coming together [17]. Emergent behaviour is, therefore, often unplanned and evolves through the interactions and collaborations that naturally develop within the SoS [23]. Interoperability can be described as the ability of two or more systems or elements to use and exchange information, thus being an important element of a SoS successful system integration [25]. However, human factors within the complex interaction between systems of the SoS requires attention, as compatible technology alone may not achieve interoperability [26]. Success can only be achieved if the stakeholder engagement is conducted correctly with all relevant stakeholders [27] throughout the SoS life-cycle.

SoSs risks and mitigations focus on desired capabilities and undesirable emergent behaviours of the SoS, and other security-related aspects along the communication channels between systems and the external world [28]. SoS capability security may be impacted by operational use or change over time, or from system-level changes to meet individual needs of constituent system stakeholders, changing risk equations that might go unidentified [29]. Security must be designed into the systems with a concious aspect towards how it is operated [30]. Applying security to systems in isolation may lead to incorrect areas of focus for effective security, potentially consuming needed resources [31], and can lead to unidentified areas of threat [9]. Other security risk may arise from within the supply chain, thus requiring further consideration as the SoS attack surface grows, therefore software supply chain risks and assurance of security must begin to be addressed during acquisition of the development life-cycle [32].

Trust and assurance are important factors for the design and operation of a secure socio-technical system. These factors and their inter-dependencies, with intrinsic and contextual trust warranting properties should be considered at the human level as well as the technical [33]. Trust is the willingness to be vulnerable, based on the positive expectations about the actions of others [34], and it is an individual's reliance on another party under conditions of dependence and risk [35]. Whereas, trustworthiness is defined from the trustor and trustee perspectives as an objective quality governing the degree to which transactional obligations will be fulfilled in situations characterised by risk or uncertainty [36]. Moreover, trustworthiness of the flow of information, the security of the service provision, and the protection of the supporting systems of the SoS need to be taken into account [37]. Capturing the criticality of independent system requirements that accurately reflect users' needs is crucial to the success of engineering and its role in the system development process [38][39]. Difficulty may increase with complexity of multiple independently managed systems and requirements that need to be co-ordinated in order to achieve the SoS objectives [17].

C. SoS and Requirements Engineering

For SoSs, the bridge between operations and requirements engineering is essential to reduce security risk against mission outcomes. Security risk assessment is applied at the operational level, carried through to the development life-cycle, where security requirements should begin with asset analysis and the context in which they are in [40] and continue to focus on related human factors and interoperability critical for the SoS operation. The emerging field of System of Systems Engineering (SoSE) requires continued growth to evolve, extending its approach beyond a single system framework towards a class of complex systems whose constituents are themselves complex [18][24]. Example approaches may include systems, security and SoSE guides [21][41][42], and other engineering approaches such as Security Quality Requirements Engineering (SQUARE) [43], various iterations of the V-Model and Double-V model for SoSE, or the Wave model for security engineering [29][44][45]. The Ministry of Defence and Department of Defense Architectural Frameworks DODAF and MODAF can also provide a means to model, understand, analyse and specify capabilities, systems, SoS and related business processes of an enterprise architecture [46].

Engineering for SoSs is driven by stakeholders' goals and needs, and involves more stakeholders than typical single-system focused systems engineering. For example, stakeholders at the system and SoS level, each have their own needs and objectives, and competing stakeholders' interests and goals [39]. Security risks will likely increase where stakeholders are not always recognised across the SoS, or stakeholders of individual systems may have little interest, or resist the SoS demands on their system giving lower priority to the SoS [47]. Stakeholders and users may have differing perceptions of different threats or risks; these can be considered with use

of heuristics, biases, mental models and distributed cognition models [48][49]. Although, where people accurately perceive security risks, they are more likely to act appropriately [50].

When modelling any system, it is useful to identify what the systems does, its purpose, mission and goals, and explore the interactions of different decisions in a security context. Models can help reflect these socio-technical characteristics [39]. However, it is also time-consuming and expensive to maintain model consistency as changes are made [14]. When modelling SoSs, a combination of top-down and bottom-up processes can be used within the requirements engineering approach, but would require modelling of goals in the system and SoS context [39]. Eventually, it may become impossible to understand the situation in its entirety [51], further suggesting the unlikelihood of a single model successfully capturing multiple dimensions and perspectives of SoSs [52]. There is a need for better models visualising how various people approach a security task, their mental models or security-related skills and knowledge. Current informal and implicit models of people are not always robust enough or rarely focus on how people make security decisions [53]. Moreover, there is a need to model a level of traceabilty and dependencies between a systems needs, risk and security requirements across the SoS as a whole [54].

Determining threats, potential areas of weakness and modelling of such instances may incorporate threat model tools e.g. [55][56][57], supported by other standard approaches for risk assessment and requirements. Various activities can also be mapped with use and misuse cases to provide a source of security requirements [58][59] that could be further combined with data-flow diagrams (DFDs) to address security concerns and risk relating to the process, storage and transmission of SoS data. Other sources of security requirements may be visualised through use of UML approaches, such as the Systems Modeling Language (SysML), Secure Tropos, UMLSec and SecureUML [60][61][62]. The Goal-oriented Requirement Language (GRL) models could be used towards considering interoperability in SoSs to examine the impact of changing system assets, goals, or user processes [63] or conflicting security and regulatory requirements [64]. Goal modelling can also be interlinked with obstacles as a form of threat modelling to visualise where threat obstacles create a risk of the goal not being achieved, usually resulting in a negative impact [65]. Although this approach could be used to derive early requirements and expectations [66], it could also be aligned when modelling risk assessment data.

There are a range of modelling tools or approaches, but limited tool-support integrating some of these different modelling elements to visualise and assess the security consequences in greater detail. As many current tools are used or designed in a single system context, identifying and integrating combinations of tool elements to suitably visualise these elements in a SoS context becomes the research challenge across independent and interdependent socio-technical system interactions of a SoS. The open-source Computer Aided Integration of Requirements and Information Security (CAIRIS) requirements management tool [67] already integrates a number of these elements and models. CAIRIS and its automatic analysis and visualisation capabilities can assist when modelling the socio-technical interaction of the SoS and the usability, security, and requirements engineering activities. This provides a view on security risks and associated assets, roles, goals, tasks, and other security and usability concepts [65]. To test the feasibility of using CAIRIS to assist the risk assessment process, CAIRIS was introduced into work discussed in Section V.

V. Research Contributions

A. Towards RQ1

RQ1 was primarily addressed through literature reviews, then supported by a case-study and related interviews to identify contributing factors and potential challenges for assessing security risk assessment of SoSs. Characterising a SoS is an important step, however each SoS can be quite different, therefore appreciating these differences and challenges that emerge will be of consideration. Given the evident differences and complexities of SoSs, we tested a process for eliciting, modelling and characterising a SoS using a candidate case-study as an Acknowledged SoS – The *Afghan Mission Network* (AMN). Further details of this work can be found in [1]. By considering the structure, management, and participation of systems and stakeholders within the SoS, this contribution helped to identify relevant human factor implementation and operational considerations, and where dependencies, constraints, or conflicting security requirements may exist towards the SoS achieving its SoS mission goals.

The approach for defining and characterising a SoS was recently extended further to ground the SoS concept, definition and description, acting as a baseline for future research undertaken. A method was proposed to simply describe the systems and SoS context, as research has found stakeholders are unclear of the SoS term or concept. The characterisation process was adapted to consider and define all main types of SoS, helping us to ask important high-level questions within the process to determine some of the scale and complexities of the SoS that can translate into the security risk and requirements process. Further details of this work can be found in [3]. This was tested in more recent work with a SoS exemplar of a Military medical evacuation (MEDEVAC) and is discussed further in pending publications also addressing RQ2 and RQ3.

B. Towards RQ2 and RQ3

Although RQ2 and RQ3 aim to achieve different objectives, we have come to find the two have symmetry and ultimately align. Findings from RQ1 and the AMN gave direction towards SoS challenges that provided the identification of important concepts to be considered within a framework for SoS security risk assessment. To explore concepts suitable to support a framework for SoS security risk assessment integrating modelling with tool-support, we implemented a SoS case-study – The *SmartPowerchair*. We tested three SoS concepts to identify how they can be considered within the security risk assessment of the SoS and their effect. Using this output with other SoS

information, this provided an opportunity to integrate the use of tool-support, testing the feasibility of CAIRIS to model the SoS and its human interactions to identify and address challenges to security risk and requirements within the SoS. Further details of this work can be found in [2].

Current work combines progress and findings from all RQs and case-studies by first defining a SoS as described in [3], then implementing a reduced-scale exemplar of a Military medical evacuation (MEDEVAC) SoS case-study using an enhanced version of OCTAVE Allegro (OA) with certain SoS elements to assess security risk. Output from OA can then be modelled using tool-support from CAIRIS, testing different means and model combinations to reflect human and system interactions leading to security risk in the SoS from which mitigations and requirements can be deduced. This provides further alignment of RQ2 and RQ3 giving direction to future work. Details of this work will be discussed in pending or future publications.

VI. Summary and Next Steps

Over the forty or more years to present day since the idea of SoS was conceived, SoSs have changed considerably. Work addressing RQ1 in particular found the term *System of Systems* can be used inconsistently, usually resulting from differences in scale, complexity, organisational and geographical boundaries, or the number of system interconnections of the SoS. Boundaries crossover many domains, such as land, sea, air, space and cyber, networks, the physical or electronic realms, cultural, organisational or geographical and environmental. These are all constrained by changing trust equations, and legal and regulatory requirements, creating different challenges for SoS security risk and requirements. For example, we identified the likelihood of unknown or unavailable risk-based information in which to base risk assessment on in some SoS types. Therefore, understanding what the minimum level of information is required to make a satisfactory security risk assessment is of importance, certainly when translating these into security requirements for the systems and SoS.

Addressing all RQs, our case-study work has considered the diversity of small and large-scale SoS examples in the present day, each with very different context, scale and complexity, governance, management and control. However, to help reduce unaccounted security risk and mitigating controls or requirements, system interconnections and stakeholder needs of the SoS need to be understood. Therefore, providing further alignment with RQ2 and RQ3, we have tested an approach using the modified OA for SoS with CAIRIS, for which we refer to as OASoSIS that aims to provide a repeatable process assisting the security risk and requirements process.

The OASoSIS approach will continue to be refined using MEDEVAC, then later implemented and tested as part of the SQUARE [43] method for the risk assessment of Step 5, whilst capturing information for Steps 1-4. CAIRIS will continue as tool-support to elicit, model, and visualise security risks, producing security requirements as an output. The more refined process will then be tested with an operational healthcare SoS or other related case-studies and subsequent publications to further validate our approach. This aims to identify the alignment of SoS factors and concepts suitable for eliciting, analysing, validating SoS security risks and requirements using tool-support, supporting decision making for the SoS and Security Requirements Engineering communities.

References

[1] D. Ki-Aries, S. Faily, H. Dogan, and C. Williams, "Re-framing The AMN: A Case Study Eliciting and Modelling a System of Systems using the Afghan Mission Network," in *11th IEEE International Conference on Research Challenges in Information Science 10-12 May 2017 Brighton, UK*. IEEE, May 2017.

[2] D. Ki-Aries, H. Dogan, S. Faily, P. Whittington, and C. Williams, "From Requirements to Operation: Components for Risk Assessment in a Pervasive System of Systems," in *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)-Proceedings of 4th International Workshop on Evolving Security & Privacy Requirements Engineering*. IEEE, 2017, pp. 83–89.

[3] D. Ki-Aries, S. Faily, H. Dogan, and C. Williams, "System of systems characterisation assisting security risk assessment," in *IEEE 13th System of Systems Engineering Conference 19 June-22 April 2018 Paris, France. IEEE.* IEEE, Jun. 2018.

[4] British Standards Institution, "BS ISO/IEC 27005, Information technology - Security techniques - Information security risk management." 2011.

[5] G. Stoneburner, A. Y. Goguen, and A. Feringa, "SP 800-30. Risk Management Guide for Information Technology Systems," Gaithersburg, MD, United States, Tech. Rep., 2002.

[6] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *computers & security*, vol. 38, pp. 97–102, 2013.

[7] R. Kissel, "Glossary of key Information Security terms," *NIST Interagency Reports NIST IR*, vol. 7298, no. 3, 2013.

[8] SANS, "Information Security Resources [online]," SANS Institute, 2015, available From: https://www.sans.org/information-security/ [Accessed 20 May 2016].

[9] R. OBrien, "Privacy and security: The new European data protection regulation and its data breach notification requirements," *Business Information Review*, vol. 33, no. 2, pp. 81–84, 2016.

[10] C. Everett, "A risky business: ISO 31000 and 27005 unwrapped," *Computer Fraud & Security*, vol. 2011, no. 2, pp. 5–7, 2011.

[11] A. Jones, "A framework for the management of information security risks," *BT technology journal*, vol. 25, no. 1, pp. 30–36, 2007.

[12] NIST, "NIST Special Publications [online]," NIST Computer Security Resource Centre, 2017, Available From: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 22 April 2017].

[13] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the information security risk assessment process," DTIC Document, Tech. Rep., 2007.

[14] I. Sommerville, *Software Engineering*, 10th ed. Pearson, 2015.

[15] R. Staker, "Decision support for complex systems-of-systems," in *Proceedings of the 16th National Conference of the Australian Society for Operations Research*. Citeseer, 2001.

[16] I. Sommerville, D. Cliff, R. Calinescu, J. Keen, T. Kelly, M. Kwiatkowska, J. Mcdermid, and R. Paige, "Large-scale complex IT systems," *Communications of the ACM*, vol. 55, no. 7, pp. 71–77, 2012.

[17] V. Chiprianov, L. Gallon, M. Munier, P. Aniorte, and V. Lalanne, "Challenges in Security Engineering of Systems-of-Systems," in *Troisième Conférence en IngénieriE du Logiciel*, 2014, p. 143.

[18] M. Jamshidi, *System of systems engineering: innovations for the twenty-first century*. John Wiley & Sons, 2011, vol. 58.

[19] J. A. Lane and D. Epstein, "What is a System of Systems and why should I care?" *University of Southern California*, 2013.

[20] D. DeLaurentis, "Role of Humans in complexity of a System-of-Systems," in *International Conference on Digital Human Modeling*. Springer, 2007, pp. 363–371.

[21] Director of Systems Engineering, *Systems Engineering Guide for Systems of Systems: Summary*, Department of Defense, Office of the Director, Defense Research and Engineering, Washington, D.C., Dec. 2010.

[22] H. Dogan, S. A. Pilfold, and M. Henshaw, "The role of Human Factors in addressing Systems of Systems complexity," in *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on*. IEEE, 2011, pp. 1244–1249.

[23] M. W. Maier, "Architecting principles for systems-of-systems," in *INCOSE International Symposium*, vol. 6, no. 1. Wiley Online Library, 1996, pp. 565–573.

[24] J. S. Dahmann and K. J. Baldwin, "Understanding the current state of US defense systems of systems and the implications for systems engineering," in *Systems Conference, 2008 2nd Annual IEEE*. IEEE, 2008, pp. 1–7.

[25] Institute of Electrical and Electronics Engineers (IEEE), *Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*, IEEE, New York, NY, 1990.

[26] Homeland Security, "The System of Systems Approach for Interoperable Communications [online]," 2017, Available From: http://www.npstc.org/download.jsp?tableId=37&column=217&id=2458&file=SOSA pproachforInteroperableCommunications_02.pdf [Accessed 4 October 2017].

[27] I. Böröcz, "Risk to the Right to the Protection of Personal Data," *European Data Protection Law Review*, vol. 2, no. 4, pp. 467–480, 2016.

[28] B. Zhou, O. Drew, A. Arabo, D. Llewellyn-Jones, K. Kifayat, M. Merabti, Q. Shi, R. Craddock, A. Waller, and G. Jones, "System-of-systems boundary check in a public event scenario," in *System of Systems Engineering (SoSE), 2010 5th International Conference on*. IEEE, 2010, pp. 1–8.

[29] J. Dahmann, G. Rebovich, M. McEvilley, and G. Turner, "Security Engineering in a System of Systems environment," in *Systems Conference (SysCon), 2013 IEEE International*. IEEE, 2013, pp. 364–369.

[30] J. R. Laracy and N. G. Leveson, "Apply STAMP to critical infrastructure protection," in *Technologies for Homeland Security, 2007 IEEE Conference on*. IEEE, 2007, pp. 215–220.

[31] K. Baldwin, J. Dahmann, and J. Goodnight, "Systems of Systems and Security: A Defense Perspective," *Insight*, vol. 14, no. 2, pp. 11–14, 2011.

[32] S. Boyson, "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems," *Technovation*, vol. 34, no. 7, pp. 342–353, 2014.

[33] I. Fléchais, J. Riegelsberger, and M. A. Sasse, "Divide and Conquer: The role of trust and assurance in the design of secure socio-technical systems," in *Proceedings of the 2005 workshop on New security paradigms*. ACM, 2005, pp. 33–41.

[34] D. E. Zand, "Trust and managerial problem solving," *Administrative science quarterly*, pp. 229–239, 1972.

[35] S. C. Currall and T. A. Judge, "Measuring trust between organizational boundary role persons," *Organizational behavior and Human Decision processes*, vol. 64, no. 2, pp. 151–170, 1995.

[36] B. P. Bailey, L. J. Gurak, and J. A. Konstan, "Trust in cyberspace," *Human factors and Web development*, pp. 311–21, 2003.

[37] C. Richardson, "Bridging the air gap: an information assurance perspective," Ph.D. dissertation, University of Southampton, 2012.

[38] C. Ncube, S. L. Lim, and H. Dogan, "Identifying top challenges for international research on requirements engineering for systems of systems engineering," in *Requirements Engineering Conference (RE), 2013 21st IEEE International*. IEEE, 2013, pp. 342–344.

[39] S. AlhajHassan, M. Odeh, and S. Green, "Aligning systems of systems engineering with goal-oriented approaches using the i* framework," in *Systems Engineering (ISSE), 2016 IEEE International Symposium on*. IEEE, 2016, pp. 1–7.

[40] D. G. Firesmith, "Analyzing and specifying reusable security requirements," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep., 2003.

[41] International Council of Systems Engineering, *Systems Engineering Handbook*, version 3.1 ed., INCOSE, Aug. 2007.

[42] R. Ross, M. McEvilley, and J. C. Oren, "Systems Security Engineering," *NIST Special Publication*, vol. 800, p. 33, 2016.

[43] N. R. Mead and T. Stehney, *Security quality requirements engineering (SQUARE) methodology*. ACM, 2005, vol. 30, no. 4.

[44] J. O. Clark, "System of Systems Engineering from a Standards V-Model and from a Standards, V-Model, and Dual V-Model Perspective," in *Systems and Software Technology Conference*, Apr. 2009.

[45] T. Weilkiens, J. G. Lamm, S. Roth, and M. Walker, *Model-based system architecture*. John Wiley & Sons, 2015.

[46] MODAF Partners, *MOD Architectural Framework Acquisition Community of Interest Deskbook*, 0th ed., The Ministry of Defence, Jul. 2005.

[47] f. A. Office of the Deputy Under Secretary of Defense, S. Technology, and S. Engineering, *Systems and Software Engineering. Systems Engineering Guide for Systems of Systems*, 1st ed., Washington, DC: ODUSD(A&T)SSE, 2008, 2008.

[48] A. M'manga, S. Faily, J. McAlaney, and C. Williams, "Folk Risk Analysis: Factors Influencing Security Analysts Interpretation of Risk," 2017.

[49] ——, "System Design Considerations for Risk Perception," 2017.

[50] K. Parsons, A. McCormac, M. Butavicius, and L. Ferguson, "Human Factors and Information Security: Individual, culture and security environment," Tech. Rep., 2010.

[51] H. De Bruijn and P. M. Herder, "System and actor perspectives on sociotechnical systems," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 39, no. 5, pp. 981–992, 2009.

[52] Y. Y. Haimes, "Risk Modeling of Interdependent Complex Systems of Systems: Theory and Practice," *Risk Analysis*, 2017.

[53] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[54] A. Nhlabatsi, T. Thun, N. Khan, Y. Yu, A. Bandara, K. Khan, and B. Nuseibeh, "Traceability for adaptive information security in the cloud," in *Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on*. IEEE, 2014, pp. 958–959.

[55] OWASP, "Threat Risk Modeling [online]," 2017, Available From: https://www.owasp.org/index.php [Accessed 1 September 2017].

[56] A. P. Moore, R. J. Ellison, and R. C. Linger, "Attack modeling for information security and survivability," Carnegie Mellon University Pittsburgh PA Software Engineering Inst., Tech. Rep., 2001.

[57] S. Faily, J. Lyle, C. Namiluko, A. Atzeni, and C. Cameroni, "Model-driven architectural risk analysis using architectural and contextualised attack patterns," in *Proceedings of the Workshop on Model-Driven Security*. ACM, 2012, p. 3.

[58] G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," *Requirements engineering*, vol. 10, no. 1, pp. 34–44, 2005.

[59] X. P. Mai, A. Goknil, L. K. Shar, F. Pastore, L. C. Briand, and S. Shaame, "Modeling security and privacy requirements: a use case-driven approach," *Information and Software Technology*, 2018.

[60] J. A. Lane and T. Bohn, "Using SysML modeling to understand and evolve systems of systems," *Systems Engineering*, vol. 16, no. 1, pp. 87–98, 2013.

[61] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt, "A comparison of security requirements engineering methods," *Requirements engineering*, vol. 15, no. 1, pp. 7–40, 2010.

[62] H. Mouratidis, "Secure software systems engineering: the Secure Tropos approach," *JSW*, vol. 6, no. 3, pp. 331–339, 2011.

[63] S. Faily and I. Fléchais, "Eliciting and Visualising Trust Expectations using Persona Trust Characteristics and Goal Models," in *Proceedings of the 6th International Workshop on Social Software Engineering*, ser. SSE 2014. ACM, 2014, pp. 17–24.

[64] S. Ghanavati, A. Rifaut, E. Dubois, and D. Amyot, "Goal-oriented compliance with multiple regulations," in *Requirements Engineering Conference (RE), 2014 IEEE 22nd International*. IEEE, 2014, pp. 73–82.

[65] S. Faily, *Designing Usable and Secure Software with IRIS and CAIRIS*, 1st ed. Springer, 2018.

[66] P. H. Meland, E. Paja, E. A. Gjære, S. Paul, F. Dalpiaz, and P. Giorgini, "Threat analysis in goal-oriented security requirements modelling," in *Computer Systems and Software Engineering: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2018, pp. 2025–2042.

[67] S. Faily, "CAIRIS [online]," June 2017, Available from: http://cairis.org [Accessed 1 June 2017].